REMARKS

These remarks are in response to the Non-Final Office Action dated January 23, 2009 (Office Action). As this Amendment is timely filed, no fee is believed due. Notwithstanding, please charge any deficiencies, and credit any overpayments, to Deposit Account No. 24-0040.

In this Amendment, Applicant has amended claims 1, 5, 9, 12, 16, 18, and 20 in this application. Applicant is not conceding that the subject matter encompassed by claims 1, 5, 9, 12, 16, 18, and 20, prior to this Amendment, is not patentable over the art cited by the Examiner. Claims 1, 5, 9, 12, 16, 18, and 20 were amended in this Amendment solely to facilitate expeditious prosecution of the application. Applicant respectfully reserves the right to pursue claims, including the subject matter encompassed by claims 1, 5, 9, 12, 16, 18, and 20, as presented prior to this Amendment, and additional claims in one or more continuing applications.

Support for these amendments can be found at least in paragraphs 5 and 19 and in FIG. 4 of Applicant's specification. No new matter has been added. Claims 4, 27, and 21 were cancelled by prior amendment. Accordingly, claims 1-3, 5-16, 18-20, and 22 are pending in the application.

Within these remarks more than one claim or more than one element from different claims may be addressed concurrently. This treatment of claims and/or elements of claims is solely to track the manner in which the rationale for rejecting the claims is set forth in the Office Action, e.g., where similar or the same citations are applied against more than one element from different claims. Though one or more elements of different claims may refer to similar or the same subject matter, the concurrent treatment of, or use of the same reasoning in support of, two or more claims and/or elements of different claims does not, in and of itself, imply that such claims and/or elements refer to the same subject matter or recite the same feature.

Telephonic Interview

Applicant would like to acknowledge, with appreciation, Examiner Moran for participating in the telephonic interview conducted on December 15, 2008. During that interview, claim 1 was discussed with reference to the cited art.

35 U.S.C. § 103 Rejections

Claims 1-3, 5-16, 18-20, and 22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,981,153 to Pang et al. (Pang) in view of U.S. Patent No. 6,496,971 to Lesea et al. (Lesea) in further view of U.S. Patent No. 5,991,858 to Weinlander (Weinlander).

Regarding claim 1, the Office Action concedes that the combination of Pang and Lesea does not disclose that:

> the decryptor is a software decryptor stored in a memory and executed by the microcontroller, wherein the system further comprises hardware that selectively enables access to the key storage register by allowing the microcontroller access when a program counter of the microcontroller specifies an address within an address range corresponding to the software decryptor within the memory.

It is asserted, however, that Weinlander discloses this aspect of claim 1.

Claim 1 has been amended to recite the following:

> wherein the decryptor is a software decryptor stored in a memory and executed by the microcontroller, wherein the system further comprises hardware, independent of the microcontroller, that allows the microcontroller access to the key storage register by unblocking a signal path coupling the microcontroller and the key storage register when a program counter of the microcontroller specifies an address within an address range corresponding to the software decryptor within the memory and disallows the microcontroller access to the key storage register by blocking the signal path coupling the microcontroller and the key storage register.

The amendments to claim 1 clarify that the hardware that regulates access to the key storage register is independent of the microcontroller. Further, the

amendments clarify that the manner in which access by the microcontroller to the key storage register is controlled is by blocking or unblocking a signal path between the microcontroller and the key storage register. Whether the signal path is blocked or unblocked is conditioned upon the address specified by the program counter of the microcontroller.

While Weinlander discloses that access to memory can be predicated upon the value of a program counter, the manner in which access to memory by the processor is controlled differs from that recited in claim 1. In particular, whereas claim 1 refers to the use of hardware that is independent of the microcontroller, Weinlander uses the processor exclusively to effectuate control. Further, whereas claim 1 recites that an actual signal path is blocked or unblocked, Weinlander uses microcode routines to suppress execution of standard commands that, if executed, access restricted memory. The execution of microcode to suppress particular commands occurs entirely within the processor.

For example, at column 2, lines 20-26, Weinlander states:

> The object is achieved by, first of all, the processor being adapted, in particular with respect to the internal microcode, in such a way that the execution of standard commands of the processor which are loaded in a user memory area and request reading or writing access to the content of memory cells is inhibited.

At column 4, lines 37-39, Weinlander recites "a processor, the processor operating in accordance with a code so as to inhibit execution of processor standard commands." Also in column 4, at lines 49-59, Weinlander recites:

> when a processor standard command loaded in the at least one user memory area requests access to a memory cell, an operating system program routine is called, the program routine checks the memory area access table to determine whether the access requested by the processor standard command lies within the authorized address area, and the program routine inhibits the execution of the processor standard command if the access requested does not lie within the authorized address area.

At column 6, lines 5-12, which were cited by the Office Action, Weinlander recites "the program routine compares the access requested by the requesting processor standard command to the authorized address area entry, contained in the memory area access table, for the requesting processor standard command."

These excerpts support the contention that Weinlander does not utilize hardware that is independent of the processor to block or unblock a signal path between the processor and the memory. As illustrated, the microcode routines are executed within the processor to suppress or inhibit the execution of standard commands that, if executed, would access some restricted portion of memory. In this regard, Weinlander discloses a system that functions differently than the system recited in claim 1.

Further illustrating the difference between claim 1 and Weinlander is that the microcode routines disclosed, in general, would be created and included in the processor when the processor is designed. That is, microcode generally is not editable by an end user or one that codes "standard" software. The solution proposed by Weinlander requires specialization within the processor itself, thereby preventing application of Weinlander to general-purpose processors that are unequipped with the microcode routines. This is not the case with the system recited in claim 1.

In addition, the obstruction of a data path coupling the microcontroller and the key storage register, as recited in claim 1, provides a physical obstruction, and thus, greater security in preventing access to the key storage register than is accomplished by Weinlander. For example, the system recited in claim 1 can overcome situations in which an instruction that accesses the restricted memory is inadvertently executed due to some form of malicious attack since the key storage register is not physically accessible by the microcontroller.

Thus, Weinlander does not disclose a mechanism for controlling whether a microcontroller is able to access a key storage register as recited in claim 1. One addressing the problem solved by Applicant's claims would not turn to Weinlander for a solution as it extensively relies upon execution of microcode in lieu of blocking a signal path.

Finally, blocking or unblocking of the signal path coupling the microcontroller and the key storage register differs from other approaches that seek to reset a processor to prevent code execution. Resetting a processor to prevent execution of an instruction that would access a restricted portion of memory can be disruptive to a system. Such disruptions can render the device vulnerable to security breaches that can compromise a secure circuit design stored within the integrated circuit.

Independent claims 9, 12, 18, and 20 include one or more features similar to those discussed above and have been rejected under similar rationale. Claims 9, 12, 18, and 20 are believed to be non-obvious over the combination of Pang, Lesea, and Weinlander for at least the reasons set forth above.

The remaining claims rejected under the combination of Pang, Lesea, and Weinlander are believed to be allowable in view of their own merits and further by virtue of their dependence upon underlying base claims.

Accordingly, withdrawal of the withdrawal of the 35 U.S.C. § 103(a) rejection of claims 1-3, 5-16, 18-20, and 22 is respectfully requested.

CONCLUSION

All claims should be now be in condition for allowance and a Notice of Allowance is respectfully requested.

If there are any questions, Applicants' attorney can be reached at Tel: 408-879-6149.

Respectfully submitted,

Michael R. Hardaway
Attorney for Applicant
Reg. No. 52,992

I hereby certify that this correspondence is being filed via EFS-Web with the United States Patent and Trademark Office on April 15, 2009.

Susan Wiens

Susan Wiens